

Security & Identity Management

CON●ECT
INFORMUNITY

Dienstag, 19. September 2006
8.00 – 18.30 Uhr

Palais Eschenbach, Festsaal
1010 Wien, Eschenbachgasse 11

- Risikomanagement / Wirtschaftskriminalität / Recht
- Standards & Normen (27 000, ITIL, u. a.)
- Operationales Sicherheitsmanagement
 - Identity Management
 - Sicherheit von Web Applikationen
 - Mobile Security / Voice Security
 - Physikalische Sicherheit
- Anwenderberichte der BAWAG zu Phishing und des Bundesministeriums für Inneres

Referenten: Helmut Deuter (RSA Security), Gerhard Göschl (Microsoft Österreich GmbH), Rainer Hörbe (BEKO), Oswald Kessler (BMI Sekt. IV – Support Unit ZMR), Robert Krickl (BAWAG), Walter Lender (Visonys IT-Security Software GesmbH), Ramon Mörl (itWatch GmbH), Christian Nordberg (Hule/Bachmayr-Heyda/Nordberg Rechtsanwälte GmbH), Karl Pfisterer (mobilkom austria), Eduard Populorum (BEKO), Enno Rey (ERNW Enno Rey Netzwerke GmbH), Peter Rogy (schoeller network control), Thomas Rothen (Microsoft Österr. GmbH), Klaus Schindelwig (TILAK GmbH), Peter Schober (CIS Certification & Information Security Services GmbH), Bozidar Sinakijevic (austria.info systems GmbH), Helmut Walkner (Siemens AG Österreich), Josef Weber (Telekom Austria AG)

Moderation: Peter Fischer (Berater), Edmund Lindau (COMPUTERWELT), Otto Zatschek (Sphinx Managed Services GmbH)

Mit freundlicher
Unterstützung
von:



Agenda

8.00 Registration

8.15 Begrüßung durch Vertreter des ASF, des Future Networks und der Computerwelt

SICHERHEITSMANAGEMENT & STANDARDS & RECHT

8.30 Information-Security-Optimierung nach ISO 27001: Von der Implementierung zum Zertifikat

Peter Schober (CIS Certification & Information Security Services GmbH)
Josef Weber (Telekom Austria AG)

9.00 Die Sicherheit des Unternehmens liegt in Ihren Händen!

Christian Nordberg (Hule/Bachmayr-Heyda/Nordberg Rechtsanwälte GmbH)
Helmut Walkner (Siemens AG Österr.)

OPERATIONALES SICHERHEITSMANAGEMENT

9.30 Identity Management im öffentlichen Bereich

Rainer Hörbe (BEKO)

10.00 Verschiedene Einsatzmöglichkeiten starker Benutzerauthentifizierung. Enterprise Single Sign-On.

Helmut Deuter (RSA Security)
Peter Rogy (schoeller network control)

10.30 Pause

11.00 Schwachstelle Client – moderne Schnittstellen – die unterschätzte Gefahr
Ramon Mörl (itWatch GmbH)

Einsatzbericht: Polizei Bayern digitale Fotografie

Ramon Mörl (itWatch GmbH)

11.30 Überregionale elektronische Zugriffe auf Patientendaten. Ein Berechtigungsvergleich zwischen Dänemark, Deutschland und Österreich

Klaus Schindelwig (TILAK GmbH)

12.00 Mehrstufiges Security-Layer-Modell für die Erfüllung höchster Sicherheitsanforderungen in der mobilen Kommunikation

Karl Pfisterer (mobilkom austria)

12.30 Mittagspause

14.00 Sicherheit für Web-Anwendungen

Walter Lender (Visonys IT-Security Software GesmbH)

14.30 Schützen Sie Ihre Unternehmens-EDV mit den richtigen Vorgehensweisen – ITIL in der Praxis, am Beispiel des Microsoft Operations Framework (MOF)

Gerhard Göschl, Thomas Rothen (Microsoft Österreich GmbH)

15.00 Voice over IP Security

Enno Rey (ERNW Enno Rey Netzwerke GmbH)

15.30 Pause

16.00 Identity Management im österreichischen E-Government

Oswald Kessler (BMI Sektion IV – Support Unit ZMR)

16.30 Security im Internet-Banking-Bereich – wichtiger denn je am Beispiel von Phishing

Robert Krickl (BAWAG)

17.00 Physikalische Sicherheit als notwendige Voraussetzung

Bozidar Sinakijevic (austria.info systems GmbH)

17.30 Der elektronische Dienstausweis

Eduard Populorum (BEKO)

18.00 Schlussdiskussion

18.30 Ende der Veranstaltung

Viele neue Begriffe der IT machen eines klar: die IT ist heute in den meisten Unternehmen eng mit dem Geschäftserfolg verbunden. Sicherheit der IT ist kein rein technisches Thema mehr, sie ist ein geschäftsrelevanter Aspekt geworden. IT-Entscheidungsträger sind Business Manager. Ausdrücke wie IT-Governance bringen diese Verantwortung klar zur Geltung.

Risk Management und Business Continuity sind Treiber für die Anforderungen an die IT. Das erfolgreiche Umsetzen der Anforderungen erfordert Kenntnisse über die Lösungsmöglichkeiten, von den rechtlichen Rahmenbedingungen über Lösungsstrategien bis zu Produkten und deren Einsatzmöglichkeiten.

Information-Security-Optimierung nach ISO 27001: Von der Implementierung zum Zertifikat

Der weltweite Standard für Informationssicherheit ISO 27001 hält Einzug in die österreichische Wirtschaft. Welche Vorteile bringt eine ISO-Zertifizierung im Wettbewerb und für die interne Security-Optimierung? Welche Anforderungen an die Organisation sind damit verbunden? Einen Überblick über die Norm-Elemente und Schlüsselaspekte

wie Risikomanagement liefert die nationale Zertifizierungsstelle CIS aus Sicht der »obersten Instanz«. Die Telekom Austria AG hat als einer der ersten IT-Service-Provider Österreichs ein Infor-



Peter Schober
(CIS Certification & Information Security Services GmbH)

mations-Sicherheits-Management-System nach ISO 27001 implementiert und zertifizieren lassen. Aus Anwendersicht wird über die Implementierung sowie den Nutzen eines ISMS berichtet. Weiters wird dargestellt, wie andere internationale Regelwerke wie Sarbanes Oxley integriert wurden und welche Aspekte eine effektive Security-Policy umfasst.

Die Sicherheit des Unternehmens liegt in Ihren Händen!

Seit 1. Jänner 2006 ist das neue Unternehmensstrafrecht (Verbandverantwortlichkeitsgesetz) in Kraft getreten, welches eine weit reichende Haftung für Firmen vorsieht.

Aus diesem Grund ist die Sicherheit der Informationstechnologie zu einer der wichtigsten Aufgaben für das Funktionieren von Unternehmen geworden.

Firmenchefs, IT-Leiter, Securitybeauftragte und Qualitätsmanager sind heutzutage im Hinblick auf die neuen strengen Rahmenbedingungen mehr denn je gefordert, eine entsprechende Security-Lösung für Ihr Unternehmen zu finden.

Die Referenten präsentieren



Josef Weber
(Telekom Austria AG)



Christian Nordberg
(Hule/Bachmayr-Heyda/Nordberg Rechtsanwältinnen GmbH)



Helmut Walkner
(Siemens AG Österreich)

anhand von praktischen Rechtsfällen die passenden Lösungszenarien und werden in einer Doppel-conference Einblick in die Welt des Paragraphendschungels gewähren.

Identity Management im öffentlichen Bereich

Das zunehmende Angebot für Anwendungen für Bürger und innerhalb der Verwaltung ergibt die Notwendigkeit Benutzeridentitäten effektiver zu verwalten. Dadurch will man eine Entlastung bei der Benutzer- und Rechteverwaltung, erhöhte Transparenz der sicherheitsrelevanten Vorgänge haben, und auch die Benutzung durch Single Sign-On vereinfachen.

ID-Management macht die Architektur von GUI- und SOA-Anwendungen skalierbarer, und im Bereich verteilter Anwendungen sind Identity-Federation und Identity-Providing-Schlüsselfaktoren für den erfolgreiche Anwendungen.

In dem Vortrag werden die Grundkonzepte und ihre Anwendung in aktuellen E-Government-Projekten erläutert.



Rainer Hörbe
(BEKO)

Verschiedene Einsatzmöglichkeiten starker Benutzerauthentifizierung. Enterprise Single Sign-On

Das RSA SecurID-System ist im Bereich Zwei-Faktor-Benutzerauthentifizierung weltweit führend. Tausende von Unternehmen und Organisationen weltweit vertrauen ihre wertvollen Netzwerk-Ressourcen diesem System an. Über 15 Millionen Menschen auf der ganzen Welt benutzen heute RSA SecurID-Authentifikatoren für den sicheren Zugang zu VPN und Remote-Access-Applikationen, Webservern und Anwendungen, Netzwerkbetriebssystemen und vielen anderen IT-Einrichtungen. Wir verschaffen Ihnen einen Überblick über verschiedene Einsatzmöglichkeiten starker Benutzerauthentifizierung.

Unternehmen suchen nach Lösungen, die ihnen die lästige Verwaltung mehrerer Passwörter ersparen. Die bis dato am Markt verfügbaren Technologien zur Vereinfachung der Passwortverwaltung entsprechen jedoch oft nicht den Sicherheitsanforderungen. Es gibt immer noch Bedenken, dass durch nur ein zentrales Master-Passwort für alle im Unternehmen genutzten Anwendungen eine Sicherheitslücke entsteht – die quasi den Schlüssel zu wertvollen Ressourcen darstellt. Der Spagat zwischen Benutzerfreundlichkeit und Online-Sicherheit gelingt mit sicheren



Helmut Deuter
(RSA Security)



Peter Rogy
(schoeller network control)

Single Sign-On Lösungen von RSA Security für das gesamte Unternehmen.

Schwachstelle Client – moderne Schnittstellen – die unterschätzte Gefahr

Schnittstellen wie USB, Infrarot, PCMCIA, Bluetooth und WLAN ermöglichen durch die Plug-and-play-Technologie dem Anwender ohne Schwierigkeiten externe Geräte an PCs und Laptops anzuschließen. Illegalen Datenaustausch, abgehörte Passwörter oder für fremde zugängliche Netzwerkzugänge sind die Folge.

Kostendruck und Innovationsdruck führen in den IT-Umgebungen des Mittelstandes und der Großunternehmen zunehmend zum Einsatz von verschiedenen Peripheriegeräten. Geschah dies bisher durch die »Hintertür«, um spontan aufkommenden Bedarf zu bedienen, so erfordert diese Technologie für den längerfristigen Einsatz zwingend ein durchdachtes, werkzeugunterstütztes Management. Die drei Facetten Sicherheit, System Management und Usability unter einen Hut zu bringen ist dabei nicht ganz einfach. Mit der Produktpalette DeviceWatch, XRayWatch, PDWatch, DEvCon steuern Sie alle Anforderungen an ein sicheres Device Management zentral.

Einsatzbericht Polizei Bayern digitale Fotografie

Das Projekt »Digitale Fotografie« der Bayerischen Polizei realisiert die Einsparpotenziale neuer Technologien, wie z. B. digitaler Kameras. Die teuren



Ramon Mörl
(itWatch GmbH)

Verfahren der traditionellen Fotografie gehören zumindest in Bayern nun der Vergangenheit an. Bayern ist mit diesem Ansatz Vorreiter und definiert damit Standards, die nicht nur in der Polizeiarbeit sondern auch in vielen Behörden und Wirtschaftsunternehmen sehr nützlich sein werden. Aus diesem Grunde sind die Schlüsselfaktoren des Projekts »Digitale Fotografie«, wie z. B. Integration in automatisierte Prozesse und inhaltliche Überprüfung der ausgetauschten Dateien, hier herausgearbeitet und die Schlüsselrolle, die damit dem Produkt DeviceWatch (www.DeviceWatch.de) zukommt, genauer beschrieben.

Überregionale elektronische Zugriffe auf Patientendaten. Ein Berechtigungsvergleich zwischen Dänemark, Deutschland und Österreich

»Der behandelnde Arzt soll jederzeit von jedem Ort auf jene Patientendaten Zugriff haben, die er für die Behandlung braucht. Dies bewirkt eine höhere Behandlungsqualität, verringert unnötige Doppeluntersuchungen und führt damit zu einer höheren Patientenzufriedenheit.«

Von solch einem Ansatz ausgehend, wurden innerhalb der letzten Jahren zahlreiche Projekte in der EU gestartet, welche eine überregionale elektronische Gesundheitsakte (ELGA) zum Ziel haben. Der Beitrag soll kritisch hinterleuchten, welche Sicherheitskonzepte zur Gewährung des Datenschutzes der Patienten dabei von verschiede-



Klaus Schindelwig
(TILAK GmbH)

denen Mitgliedsstaaten zugrunde gelegt wurden und wie erfolgreich diese Projekte sind.

Mehrstufiges Security-Layer-Modell für die Erfüllung höchster Sicherheitsanforderungen in der mobilen Kommunikation

Der Einsatz mobiler Datenübertragung ist heute längst dem Bereich des mobilen Mailverkehrs entwachsen und bildet zunehmend unternehmenskritische Informationen und Prozesse ab. Dadurch sehen wir uns mit neuen Security-Anforderungen im Bezug auf mobiles Datenmanagement konfrontiert. Welche besonderen Herausforderungen dies sind und wie ein mehrstufiges Provider-Sicherheitskonzept dazu aussehen kann, wird im Zuge dieses Beitrags vorgestellt.



Karl Pfisterer
(mobilkom austria)

Die Inhalte im Überblick:

- Welche besonderen Anforderungen an Security ergeben sich aus dem Kontext der mobilen Datenkommunikation?
- mobilkom austria stellt sein dreistufiges Provider Sicherheitskonzept vor, das für die unterschiedlichsten Anwendungsfälle eine optimale Abdeckung auch höchster Securityanforderungen gewährleistet.
- Die drei Security Layer sind: Netzsicherheit/sichere mobile Plattformen/modernste Verschlüsselungstechnologien als Add-ons für bestehende mobilkom-Produkte.

Sicherheit für Web-Anwendungen

Bisher wird »Web Application Security« häufig ausschließlich unter dem Gesichtspunkt der fehlerhaften Programmierung und Konfiguration gesehen aber manipulierte HTTP-Requests sind in der Lage, Schwachstellen auf allen Ebenen einer Web Anwendung auszunutzen. Besonders attraktiv für Angreifer ist die Tatsache, dass für einen Großteil der möglichen Attacken kein spezielles Tool benötigt wird, ein Standard-Webbrowser ist vollkommen ausreichend.



Walter Lender
(Visonys IT-Security
Software GesmbH)

Geschäftlich relevante Auswirkungen solcher Angriffe sind in der Regel:

- Zugriff auf vertrauliche Daten und Informationen
- Manipulieren und Verändern von Inhalten
- Vortäuschen einer Kunden- oder Partner-Berechtigung
- Die Anwendung wird überlastet und ist nicht mehr verfügbar

Web-Anwendungen können nur mit dem Einsatz einer Application-Firewall (auch Application-Proxy) effizient geschützt werden. Die Application-Firewall wird als Gateway zwischen externer Welt und Webserver/Webanwendung platziert und kontrolliert den gesamten HTTP-Datenstrom auf bösartige Inhalte. Ein weiterer Nutzen dieser Lösung ist, dass die laufende Beseitigung von Schwachstellen bei Webanwendungen nicht unmittelbar sofort erforderlich ist.

Schützen Sie Ihre Unternehmens-EDV mit den richtigen Vorgehensweisen – ITIL in der Praxis, am Beispiel des Microsoft Operations Framework (MOF)

Sicherheit ist komplex. Nur durch das Zusammenfügen mehrerer Schichten lässt sich ausreichende Sicherheit erzielen.

Am Beispiel des Microsoft Operations Frameworks (MOF) und durch Kunden Referenzen zeigen wir Ihnen wie sich ITIL in der Praxis umsetzen lässt.

Das Microsoft Operations Framework (MOF) stellt eine strukturierte Vorgehensweise dar, um den erfolgreichen Betrieb einer IT-Infrastruktur unter Verwendung von Microsoft-Produkten sicherzustellen.

MOF ist eine Zusammenstellung von Best Practices, Prinzipien und Modellen, die Richtlinien liefern, um Hochverfügbarkeit, Zuverlässigkeit und Sicherheit in unternehmenskritischen Produktionssystemen sicherzustellen.



Gerhard Göschl
(Microsoft Österreich
GmbH)



Thomas Rothen
(Microsoft Österreich
GmbH)

Voice-over-IP-Security

Sicherheitsprobleme von VoIP können auf verschiedenster Ebene auftreten, etwa beim Datentransport, am Endgerät oder auf Protokollebene. Der Vortrag gibt einen Überblick über den aktuellen Stand an Angriffsmethoden und Sicherheitsmaßnahmen und demonstriert praktische Attacken.



Enno Rey
(ERNW Enno Rey
Netzwerke GmbH)

Identity Management im österreichischen E-Government

Identitäten und der sichere elektronische Umgang mit diesen Identitäten ist in der heutigen mobilen Gesellschaft wichtiger denn je. Welche rechtlichen Aspekte und möglichen gesetzlichen Auswirkungen insbesondere im Lichte des Österreichischen E-Government-Konzeptes bestehen, werden in diesem Vortrag behandelt.



Oswald Kessler
(BMI Sektion IV –
Support Unit ZMR)

Security im Internet-Banking-Bereich – wichtiger denn je am Beispiel von Phishing

Das WWW wurde als die Errungenschaft des 20. Jahrhunderts gepriesen. Ohne Internet gäbe es

viele Probleme beim täglichen Geschäftsverkehr. Aber auch das organisierte Verbrechen bedient sich des Internets und versucht daraus Kapital zu schlagen. Die unterschiedlichen Angriffsmuster werden täglich mehr und auch immer besser.

- Welche Angriffe gibt es?
- Wie können wir uns davor schützen?
- Eine kurze Darstellung der derzeitigen Situation.

Physikalische Sicherheit als notwendige Voraussetzung

Bei der Suche nach einem neuen Rechenzentrum hat man sich bei der Österreich Werbung mehr Gedanken über Verfügbarkeiten, Reaktionszeiten und zuverlässige Dienstleister gemacht, als über die physikalische Sicherheit der Server. Eine Verfügbarkeit von 99,8%, USV und Notstromdiesel oder eine 24x7-Betreuung sind nicht außergewöhnlich. Trotzdem konnten nur wenige Rechenzentren die Anforderungen erfüllen. Und nur ein Rechenzentrum konnte beim Thema Sicherheit noch ein wenig mehr bieten.

Seit 1.5.2006 lässt die Österreich Werbung ihre Server im earthDATAsafe in Kapfenberg durch DaimlerChrysler Computing Services betreiben. Ausschlaggebend war, dass ein einzelnes Rechenzentrum die Verfügbarkeit eines verteilten Re-



Robert Krickl
(BAWAG)



Bozidar Sinakijevic
(austria.info systems
GmbH)

chenzentrums anbieten und trotzdem Billigstbieter sein konnte. Wie das erreicht wurde und welche Erfahrungen die Österreich Werbung mit dem earthDATAsafe gemacht hat, wird Hr. Bozidar Sinakijevic von austria.info systems darlegen.

Der elektronische Dienstaussweis

Bei den Bundesbehörden werden die bisherigen papierernen Dienstaussweise durch elektronische Dienstaussweise (eDA) ersetzt. Diese Karten im Scheckkartenformat enthalten alle optischen Merkmale, die ein Dienstaussweis oder auch ein national gültiger Personalausweis erfüllen muss um die Identität einer Person festzustellen. Diese Merkmale sind Bild, Unterschrift, Name, Geburtsdatum, dazu noch Behörde, Dienststelle und allenfalls besondere Funktionen des Karteninhabers, wie etwa der Hinweis der Autorisierung auf eine Festnahmeberechtigung.

In diesem Vortrag werden auch die vielfältigen elektronischen Funktionen und Anwendungsmöglichkeiten aufgezeigt, die es ermöglichen den Gebrauchswert des Ausweises massiv zu erhöhen.



Eduard Populorum
(BEKO)

Seminar Information-Security-Manager

Technologieexperte mit Führungsqualitäten mit Zertifizierungsprüfung nach BS 7799 / ISO 17799



Ein Technologie-Experte mit Führungsqualitäten

InformationSicherheitsManager ist ein Berufsbild mit Zukunft. Mit Ihrer Führungs- und Technologiekompetenz nehmen Sie eine zentrale Position im Unternehmen ein. Sie betreuen die Implementierung und ständige Verbesserung von ISMS und fungieren als Schnittstelle zwischen der obersten Führungsebene und den operativen Bereichen.

Entsprechend weit ist der Bogen der Ausbildungsinhalte gespannt. Der Lehrgang umfasst drei Module, die unabhängig voneinander besucht werden können:

- Die Norm ISO 17799 / BS 7799 (2 Tage)
- Psychologische Grundlagen für IS-Manager (1 Tag)
- Rechtsgrundlagen (1 Tag)

Die Teilnahme an allen drei Seminaren ist Voraussetzung für das Absolvieren der Prüfung. Der erfolgreiche Abschluss wird Ihnen mit dem staatlich anerkannten CIS-Zertifikat bescheinigt, das auch international gültig ist.

- Prüfung IS-Manager (1 Stunde)
- Zertifikat IS-Manager

Modul 1: Die IS-Norm BS 7799 / Iso 17799 Aus Risiko wird messbare Sicherheit

Dieses Zwei-Tages-Modul vermittelt Ihnen das Fundament, auf dem moderne ISM-Systeme aufbauen: die Norm ISO 17799 / BS 7799 mit allen Teilbereichen wie Security Policy, Risk Management oder Business Continuity Planning sowie auch übergeordnete Aspekte wie Organisation oder Prozessmanagement. Mittels praktischer Fallbeispiele wird die selbständige Umsetzung des Gelernten gefördert.

Modul 2: Psychologische Grundlagen für IS-Manager Soft-Skills: Gewusst wie!

Die Einführung neuer Systeme stößt leicht auf Widerstände – außer man beherrscht die hohe Schule der Psychologie. Dieses eintägige Seminar vermittelt Ihnen die Grundlagen, um das erworbene Fachwissen erfolgreich im Unternehmen umsetzen zu können. Dazu gehören Soft-Skills wie Moderationsfähigkeit, Teamfähigkeit oder Konfliktfähigkeit, aber auch Wissen über Beziehungsmodelle, gruppenspezifische Prozesse und Motivationstechniken.

Referenten:

Günther Schreiber (Quality Austria, CIS),
Herfried Geyer (Siemens Business Services),
Markus Frank (L-L.M.), **Johann Brunner** (WKO)

Modul 3: Rechtsgrundlagen für IS-Manager Gut informiert ist halb gewonnen!

Ein wichtiges Element im Bereich Informationssicherheit sind Gesetze, die den Schutz von Daten regeln. In diesem eintägigen Seminar werden Ihnen vier für Information-Security relevante Schwerpunkte vermittelt: Datenschutz, Wettbewerbsrecht, E-Commerce, Urheberrecht. Mit diesem Überblick verfügen Sie über das grundlegende Rüstzeug, um ein kompetenter Ansprechpartner für zugezogene Rechtsberater zu sein.

Termine: CB060490	11. – 14. September 2006
CB060491	13. – 16. November 2006

Ort: Wien

Gebühr: **Gesamter Lehrgang IS-Manager**
inkl. Prüfung und Zertifikat: € 3.060,-
Alle Preise zuzüglich 20% MWST.

www.conect.at

An
CON•ECT Eventmanagement
Kaiserstraße 14/2
1070 Wien

Tel.: +43 / 1 / 522 36 36-36
Fax: +43 / 1 / 522 36 36-10
E-Mail: registration@conect.at
<http://www.conect.at>

In Kooperation mit:



COMPUTERWELT



Zielgruppe:
Unternehmensleitung, Sicherheitsverantwortliche, IT-Vorstand,
IT-Entscheider, IT-Verantwortliche sowie Vertreter von Medien
und Wissenschaft

ANMELDUNG: Nach Erhalt Ihrer Anmeldung
senden wir Ihnen eine Anmeldebestätigung.
Diese Anmeldebestätigung ist für eine Teilnahme
am Event erforderlich.

STORNIERUNG: Falls Sie nach erfolgter Anmel-
dung doch nicht am Event teilnehmen können,
bitten wir Sie, uns unbedingt rechtzeitig Bescheid
zu geben, damit wir Ihren Platz an einen anderen
Interessenten weitergeben können.

ADRESSÄNDERUNGEN: Wenn Sie das Unter-
nehmen wechseln oder wenn wir Personen an-
schreiben, die nicht mehr in Ihrem Unternehmen
tätig sind, teilen Sie uns diese Änderungen bitte
mit. Nur so können wir Sie gezielt über unser
Veranstaltungsprogramm informieren.

Anmeldung

CON•ECT
EVENTMANAGEMENT

Ich melde mich zu »Security und Identity Management« am 19. 9. 2006 an:

- als IT-Anwender kostenfrei
 als IT-Anbieter / Berater zum Preis von € 390.- (+ MWSt.)

Anmeldeschluss: 17. September 2006

- Ich möchte in Zukunft weiter Veranstaltungsprogramme per E-Mail oder
Post übermittelt bekommen.

Firma:

Titel:

Vorname:

Nachname:

Funktion:

Straße:

PLZ:

Ort:

Telefon:

Fax:

E-Mail:

Datum:

Unterschrift/Firmenstempel:

● Ich erkläre mich mit der elektronischen
Verwaltung meiner ausgefüllten Daten und der
Nennung meines Namens im Teilnehmerver-
zeichnis einverstanden.

● Ich bin mit der Zusendung von Veran-
staltungsinformationen per E-Mail einverstanden.
(Nichtzutreffendes bitte streichen)